(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－329011

(43)公開日　平成８年(1996)12月13日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ			技術表示箇所
G06F 15/00	330	9364-5L	G06F 15/00	330	Z	
12/00	537	7623-5B	12/00	537	H	
17/60		7259-5J	G09C 1/00			
G09C 1/00			G06F 15/21		Z	
H04L 9/06			H04L 9/02		Z	

審査請求　未請求　請求項の数２　ＯＬ　（全10頁）　最終頁に続く

(21)出願番号　特願平7－136808

(22)出願日　平成７年(1995)６月２日

(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内２丁目６番３号

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　斎藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内

(72)発明者　岡崎　正一
神奈川県鎌倉市上町屋325番地　三菱電機株式会社情報システム製作所内

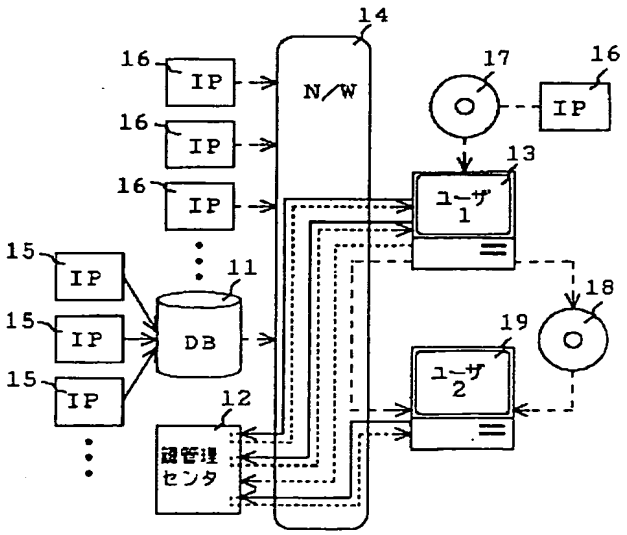
(74)代理人　弁理士　南條　眞一郎

(54)【発明の名称】データ著作権管理システム

(57)【要約】

【目的】　１次ユーザが入手したデータを加工し、加工されたデータを２次利用者へ供給するデータ著作権管理システムを提供する。

【構成】　データベース、鍵管理センタを備え、１次著作権ラベル、第１暗号鍵を含む１次利用鍵，２次利用鍵，第３暗号鍵，著作権管理プログラムが用いられる。１次ユーザは第１暗号鍵を用いて暗号化されて供給された１次著作権データを鍵管理センタから入手した１次利用鍵で平文化し利用するが、保存する場合には１次利用鍵を用いて再暗号化される。１次ユーザは鍵管理センタから１次著作権データ加工用の２次利用鍵を入手して１次著作権データの加工を行い、加工途中のデータは２次利用鍵で暗号化されて保存される。１次ユーザは加工が終了すると２次著作兼用の第３暗号鍵を鍵管理センタから受け取り、加工済みデータを第３暗号鍵で暗号化し、２次ユーザに配布する。２次ユーザは鍵管理センタから第３暗号鍵を入手し、加工データを利用する。



1

【特許請求の範囲】

【請求項１】　データベースおよび鍵管理センタを備え、データ著作物を入手した１次ユーザが入手した１次著作権データを加工し、加工によって得られた２次著作権データを２次利用者へ供給する場合に著作権を管理するデータ著作権管理システムであって：前記１次著作権データが１次利用鍵を用いて暗号化されて前記１次ユーザに供給され；前記１次著作権データの利用を希望する前記１次ユーザからの前記１次利用鍵の配布要求に対し、前記鍵管理センタが前記１次利用鍵を前記１次ユーザに配布し；前記１次ユーザは配布された前記１次利用鍵を用いて前記１次著作権データを平文化して１次利用を行い；前記１次著作権データの加工を希望する前記１次ユーザは前記鍵管理センタから前記１次著作権データを加工するための２次利用鍵の配布を受け、配布された前記第２利用鍵を用いて前記１次著作権データの加工を行い、加工中の著作権データは前記第２利用鍵を用いて暗号化されて保存され；加工が終了した前記１次ユーザは前記鍵管理センタから加工済みデータを配布するための第３暗号鍵の配布を受け、前記加工済みデータを前記第３暗号鍵を用いて暗号化して２次ユーザに供給し；前記２次著作権データの利用を希望する前記２次ユーザは前記鍵管理センタから前記第３暗号鍵の配布を受け、配布された前記第３暗号鍵を用いて前記２次著作権データを平文化して利用する；データ著作権管理システム。

【請求項２】　前記１次ユーザによる前記１次著作権データの加工が、前記１次著作権データの複写物に対して行われる請求項１記載のデータ著作権管理システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はディジタルデータの利用、すなわち表示，保存，複写，加工，転送において著作権を管理するシステムに係るものである。

【０００２】

【従来の技術】情報化時代と言われる今日、通常の地上波放送(terrestrial broadcasting)の他に放送衛星（Broadcasting Satellite：ＢＳ）、通信衛星（CommununicationSatellite：ＣＳ）と呼ばれる衛星放送、同軸ケーブルあるいは光ケーブルを利用したＣＡＴＶ（Cable Television）と呼ばれる有線ＴＶ放送が普及しつつある。

【０００３】同時に数１０チャンネルを配信することができる衛星放送あるいはＣＡＴＶ放送においては、包括的な契約によって視聴することができるスクランブルがかけられていない一般的なチャンネルの他に、包括的な契約によっては視聴することができないスクランブルされた映画・スポーツ・音楽等専門的なチャンネルが設けられている。これらのチャンネルを視聴するためにはスクランブルを解除するするために契約を行う必要があるが、この契約期間は通常１カ月程度の単位で行われるため、随時の契約によって視聴することができない。

2

【０００４】この問題に対応するために、本発明者らは特開平６－４６４１９号及び特開平６－１４１００４号で公衆電信電話回線を通じて課金センタから視聴許可鍵を入手するとともに課金が行われ、視聴許可鍵を用いて番組毎に異なるスクランブルパターンで行われたスクランブルを解除して番組を視聴するシステムを、特開平６－１３２９１６号でそのための装置を提案した。これらのシステム及び装置において、スクランブルされた番組の視聴を希望する者は通信装置を使用し通信回線を経由して課金センタに視聴申し込みを行い、課金センタはこの視聴申し込みに対して通信装置に許可鍵を送信するとともに課金処理を行い料金を徴収する。通信装置で許可鍵を受信した視聴希望者は通信装置と受信装置を接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって番組のスクランブルを解除する。

【０００５】特開平６－１３２９１６号にはこれらのシステム及び装置の応用として、各々異なるスクランブルパターンでスクランブルされた複数のデータが記録されたテープあるいはディスクを販売あるいは貸与し、ＩＣカード等により許可鍵を供給して特定のデータを利用するシステム及び装置も記載されている。

【０００６】また、情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータをＬＡＮ（Local Area Network）と呼ばれる局所的ネットワーク、ＷＡＮ（Wide Area Network）と呼ばれる国単位のネットワークさらにはこれらを国際的に拡大したインターネット（InterNet）と呼ばれるネットワークによってコンピュータ通信ネットワークシステムを構成し、相互に利用するデータベースシステムが普及しつつある。

【０００７】一方、デジタル化すると情報量が膨大になるためデジタル化することができなかったテレビジョン動画信号を圧縮することにより情報量を減少させ、実用的なデジタル化を可能にする技術が開発され、これまでにテレビジョン会議用のH.２６１規格，静止画像用のＪＰＥＧ（Joint Photographic image coding Experts Group）規格，画像蓄積用のＭＰＥＧ１（Moving Picture image coding Experts Group 1）規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するＭＰＥＧ２規格が作成された。

【０００８】これらの画像圧縮技術を利用したデジタル化技術はテレビジョン放送あるいはビデオ画像記録用に用いられるだけではなく、コンピュータでこれまで扱うことができなかったテレビジョン動画データが扱うことができるようになり、コンピュータが扱う各種のデータとデジタル化されたテレビジョン動画データを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。このマルチメディアシステムもデータ

通信に組み入れられ、データベース上のデータの一つとして利用される。

【０００９】このようにしてデータベースの利用範囲が拡大する中で、データベース上のデータ利用に対する課金をどのようにして行うかということ及びデータの直接的な利用以外の複写あるいは転送等によって発生する著作権の問題及びデータの加工によって発生する２次的著作権の問題をどのようにして処理するかということが重要になる。課金及び著作権の処理を確実に行うには、正規の利用者でなければデータの利用が不可能であるようにする必要があり、データを暗号化しておくことがそのための最良の手段である。

【００１０】これらのテレビジョンシステムあるいはデータベースシステムにおいて、データを暗号化し、暗号化されたデータを復号して利用するためには暗号鍵が必要であり、データ利用者に対して暗号鍵を渡さなければならないが、この作業は安全性及び確実性が要求されるため非常に煩雑である。

【００１１】本発明はその構成において暗号技術が重要な役割を果たすが、初めに一般的な暗号技術について説明する。暗号技術においては、平文Ｍを暗号鍵Ｋを用いて暗号化し暗号文Ｃを得る暗号化（Encryption）を

Ｃ＝Ｅ（Ｋ，Ｍ）

と表現し、暗号文Ｃを暗号鍵Ｋを用いて復号化し平文Ｍを得る復号化（Decryption）を

Ｍ＝Ｄ（Ｋ，Ｃ）

と表現する。

【００１２】さらに、本発明者らは特願平６－６４８８９号においてデータ著作権管理システムの具体的な構成を提案した。このシステムでは、ディジタル映像のリアルタイム送信も含むデータベースシステムにおけるディジタルデータの表示（音声化を含む），保存，複写，加工，転送における著作権の管理を行うために、利用申し込み者に対して暗号化されたデータの利用を許可する鍵の他に、必要に応じて著作権を管理するためのプログラム，著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を送信する。著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【００１３】また、データは暗号化されて供給され、許可鍵を用いて復号化され利用されるが、装置内への保存、装置外の媒体への複写、装置外への転送が行われる場合には暗号化される。また、表示・利用、保存、複写、加工、転送等の利用形態各々に対して許可鍵が用意される。

【００１４】

【発明の概要】本発明のシステムはデータベース、鍵管理センタ、１次ユーザ、２次ユーザおよびこれらを相互に接続するネットワークシステムから構成され、１次著作権ラベル、第１暗号鍵を含む１次利用鍵，第２暗号鍵を含む２次利用鍵，２次著作権ラベル，第３暗号鍵，著作権管理プログラムが用いられる。平文１次著作権データは１次暗号鍵を用いて暗号化された状態で、１次ユーザに供給され、暗号１次著作権データの利用を希望する１次ユーザは、鍵管理センタにネットワークシステムを経由して１次利用鍵の配布を要求し、１次ユーザからの１次利用鍵の配布要求を受けた鍵管理センタは１次利用鍵を１次ユーザに配布し、このときに課金を行う。

【００１５】１次ユーザは配布された１次利用鍵に含まれる第１暗号鍵を用いて暗号化１次著作権データを平文化し利用するが、平文１次著作権データを１次ユーザの装置内へ保存する場合には１次利用鍵を用いて再暗号化される。１次著作権データの加工を希望する１次ユーザが平文１次著作権データの加工を行うための２次利用鍵の配布をネットワークシステムを経由して鍵管理センタに要求すると、鍵管理センタは２次利用鍵を１次ユーザに配布する。２次利用鍵を受け取った１次ユーザは１次著作権データの複写を作成し、複製された１次著作権データの加工を行い、加工途中の平文２次著作権データを２次利用鍵に含まれた第２暗号鍵により暗号化し、最終加工データは第３暗号鍵を用いて暗号化して１次ユーザの装置内に保存する。１次ユーザは２次著作権データのデータ加工についての２次著作権を行使するために鍵管理センタに第３暗号鍵を登録し、暗号２次著作権データを第３暗号鍵を用いて暗号化して外部記憶媒体への複写あるいはネットワークシステムを介して転送することにより２次ユーザへ供給する。

【００１６】暗号２次著作権データの利用を希望する２次ユーザは、鍵管理センタに第３暗号鍵の配布を要求し、第３暗号鍵の配布要求を受けた鍵管理センタは、第３暗号鍵をネットワークシステムを経由して２次ユーザに配布する。２次暗号鍵を受け取った２次ユーザは２次暗号鍵を用いて暗号２次著作権データを復号し、利用する。

【００１７】

【実施例】以下、図面を用いて本発明の実施例を説明する。初めに、本発明が対象とするデータ著作権管理システムの構成を図１を用いて説明する。図１に示されたシステムはデータベース１、鍵管理センタ２、ユーザ３，３，３・・・およびこれらを相互に接続するネットワークシステム４から構成されている。また、データベース１には情報提供者（Information Provider：ＩＰ）５，５，５・・・からデータが供給されるが、場合によってはデータベース１を経由することなく情報提供者６，６，６・・・からネットワークシステム４を経由して直接にユーザ３に対してデータが供給されることがある。なお、本発明において利用するデータはプログラムとデ

ータが組み合わされてオブジェクトである。ユーザ３は単なる利用者ではなく入手した複数の著作権データを組み合わせたり、修正したりすることにより新しい著作物（２次著作物）を提供する情報提供者５あるいは６となる。

【００１８】このように構成される本発明のデータ著作権管理システムにおいて、各情報提供者５，６から提供される著作権データは著作権を保護するために暗号化されている。したがって、暗号著作権データを入手したユーザ３が利用するには暗号著作権データを復号する必要がある。そのため、このシステムにおいて暗号鍵はすべて鍵管理センタ２に預けられ、鍵管理センタ２が管理している。また、各情報提供者５，６が採用する暗号方式は自由であるが後で述べる２次利用以降で使用される暗号方式は鍵センタが採用する方式に限られる。

【００１９】データベースからのデータ利用は一般的にパーソナルコンピュータを用いて行われるが、そこで用いられるＯＳとしてはセキュリティ対応処理を組み込んでいるものを使用する必要がある。また、暗号鍵等の管理を行うために著作権管理プログラムが使用されるが、この著作権管理プログラムおよび鍵管理センタ２から受け取った暗号鍵を保管しておく必要があるため、メモリあるいはＨＤＤ上にソフトウェア的に実現されあるいは専用のボード、ＰＣカード等でハードウェアとして実現される「キーカード」がこれらの保管場所として用意される。

【００２０】鍵管理センタ２は、実際に利用されているか単に登録されているのみで利用されていないかを問わず、データ著作物の著作権の保護と著作権の利用に対する課金を行うために鍵を保管し、保管されている鍵と著作権ラベルの対応付けを行うことにより鍵の管理を行う。

【００２１】図２に示されたのは、情報提供者からデータ著作物を入手した１次ユーザが、入手したデータを加工し、加工されたデータを２次利用者へ供給する本発明のデータ著作権処理システム実施例の概要構成である。このシステムにおいては平文１次著作権データＤ1，暗号１次著作権データ（Encrypted Data）ＥＤ1i，平文２次著作権データＤ2，暗号２次著作権データＥＤ2j，平文１次著作権ラベル（Label）ＬＣ1，第１暗号鍵（Key）Ｋ1iを含む１次利用鍵Ｋ1，２次利用鍵Ｋ2，第３暗号鍵Ｋ3j，平文著作権管理プログラムＰＣが用いられる。

【００２２】このシステムはデータベース１１、鍵管理センタ１２、１次ユーザ１３、２次ユーザ１９およびこれらを相互に接続するネットワークシステム１４から構成される。また、データベース１１には情報提供者１５，１５，１５・・・からデータが供給されるが、場合によってはデータベース１１を経由することなく情報提供者１６，１６，１６・・・からネットワークシステム１４を経由してあるいは情報提供者１６からＣＤＲＯＭ等の情報記録媒体１７を介して直接にユーザ１３に対してデータが供給されることがある。なお、この図において実線で示されたのは平文データの経路、破線で示されたのは暗号データの経路、点線で示されたのは鍵の経路である。

【００２３】このシステムにおいて、平文１次著作権データＤ1iは第１暗号鍵Ｋ1iを用いて暗号化された状態で暗号１次著作権データＥＤ1iの形で、

ＥＤ1i＝Ｅ（Ｋ1i，Ｄ1i）

情報提供者１５からデータベース１１を介してネットワークシステム１４を経由して、情報提供者１６からネットワークシステム１４を経由してあるいはＣＤＲＯＭ等の情報記録媒体１７を介して１次ユーザ１３に供給される。供給された暗号１次著作権データＥＤ1iの利用を希望する１次ユーザ１３は、鍵管理センタ１２にネットワークシステム１４を経由して１次著作権ラベルＬＣ１を提示して１次利用鍵Ｋ１の配布を要求する。

【００２４】１次ユーザ１３からの１次利用鍵Ｋ1の配布要求を受けた鍵管理センタ１２は提示された１次著作権ラベルＬＣ1により１次利用鍵Ｋ1を探し出し、１次利用鍵Ｋ1をネットワークシステム１４を経由して１次ユーザ１３に配布し、このときに課金を行う。１次ユーザ１３は配布された１次利用鍵Ｋ1に含まれる第１暗号鍵Ｋ1iを用いて暗号化１次著作権データＥＤ1iを平文化し、

Ｄ1i＝Ｄ（Ｋ1i，ＥＤ1i）

利用する。

【００２５】平文１次著作権データＤ1iを１次ユーザ１３の装置内へ保存する場合には第１暗号鍵Ｋ1iを用いて再暗号化し、

ＥＤ1i＝Ｅ（Ｋ1i，Ｄ1i）

暗号化されたデータＥＤ1iが保存される。再暗号化されたデータＥＤ1iを再利用する場合には第１暗号鍵Ｋ1iを用いて再平文化および再暗号化が行われる。

【００２６】平文１次著作権データＤ1iの加工を希望する１次ユーザ１３は平文１次著作権データＤ1iの加工を行うための２次利用鍵Ｋ2の配布をネットワークシステム１４を経由して鍵管理センタ１２に要求する。

【００２７】２次利用鍵Ｋ2の配布要求を受けた鍵管理センタ１２は、２次利用鍵Ｋ2をネットワークシステム１４を経由して１次ユーザ１３に配布する。２次利用鍵Ｋ2を受け取った１次ユーザ１３は許可鍵の内容に従って平文１次著作権データＤ1の加工を行い、平文２次著作権データＤ2jを加工によって得る。平文２次著作権データＤ2jをユーザ１３の装置内に保存する場合には、第２暗号鍵Ｋ2によって暗号化される。

ＥＤ2j＝Ｅ（Ｋ2，Ｄ2j）

加工が最終的に終了すると、１次ユーザ１３は２次著作権データのデータ加工についての２次著作権を行使するために、第３暗号鍵Ｋ3jを生成し生成された第３暗号鍵

K3jを鍵管理センタ１２に登録する。なお、第３暗号鍵K3jは１次ユーザ１３ではなく鍵管理センタ１２が作成し、１次ユーザ１３からの要求により配布するようにしてもよい。

【００２８】１次ユーザ１３が平文暗号２次著作権データED2jを外部記憶媒体１８への複写あるいはネットワークシステム１４を介して転送する場合には、平文２次著作権データED2jを第３暗号鍵で暗号化し、

ED3j＝E（K3j，D2j）

２次ユーザ１９へ供給する。

【００２９】供給された暗号２次著作権データED3jの利用を希望する２次ユーザ１９は、鍵管理センタ１２にネットワークシステム１４を経由して第３暗号鍵K3jの配布を要求する。２次ユーザ１９からの第３暗号鍵K3jの配布要求を受けた鍵管理センタ１２は第３暗号鍵K3jをネットワークシステム１４を経由して２次ユーザ１９に配布する。第３暗号鍵K3jを受け取った２次ユーザ１９は、第３暗号鍵K3jを用いて暗号２次著作権データED2jを復号し、

D2j＝D（K3j，ED2j）

利用する。その場合も、暗号化データED2jを再度利用する場合には第３暗号鍵K3jを用いて復号化および暗号化が行われる。

【００３０】１次著作権データの入手、１次著作権データの１次利用、１次著作権データの加工、加工された２次著作権データの供給および２次著作権データの利用について詳細に説明する。このシステムにおいて、複数の１次著作権データD1iは１次暗号鍵K1iを用いて暗号化された状態で

ED1i＝E（K1i，D1i）

平文１次著作権ラベルLC1とともに、情報提供者１１から直接にあるいはデータベースを介して、１次ユーザ１３に供給される。

【００３１】著作権管理プログラムPCはユーザによる著作権データの使用を管理するものであり、具体的には与えられた暗号鍵を用いての著作権データの復号化及び再暗号化および利用鍵の内容に従う著作権データの利用制限を行う。このシステムにおいて提供される暗号データED1jには暗号鍵入手等に利用するための平文の１次著作権ラベルLC1が付けられており、すなわち、暗号１次著作権データED1は平文１次著作権ラベルLC1と暗号１次著作権データED1iから構成されている。平文１次著作権ラベルLC1にはデータのタイトル名，使用しているアプリケーション・プログラム名，１次著作権者名が記入されている。供給された暗号１次著作権データED1iの利用を希望する１次ユーザ１３は、鍵管理センタ１２にネットワークシステム１４を経由して平文１次著作権ラベルLC1を提示して１次利用鍵K1の配布を要求する。

【００３２】提示された１次著作権ラベルLC1により、配布すべき１次利用鍵が鍵K1であることを確認した鍵管理センタ１２は確認された１次利用鍵K1をネットワークシステム１４を経由して１次ユーザ１３に配布する。配布された１次利用鍵K1を受信した時点で１次ユーザ１３の装置は著作権管理モードになり、１次ユーザ１３は１次著作権データの利用が可能になる。なお、第１暗号鍵K1iは１次利用鍵K1に含まれているため、１次ユーザ１３から第１暗号鍵K1iは認識されない。一方、鍵管理センタ１２は課金処理を行うとともに著作権データの使用状況および１次ユーザ１３のデータベース利用状況を把握する。

【００３３】図３に示されたのは、本発明において著作権管理プログラムPCが行う１次利用の制限を説明する概念図である。先願である特願平６－６４８８９号に記載された発明と同様に、本願発明のデータ著作権管理システムにおける入手したデータの１次利用は通常の利用形態すなわちデータの直接的な利用およびその利用結果の印刷を含む出力に限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての転送及び加工、さらに原則としてデータの装置内部での保存を行うことはできない。ただし、データが暗号化されている場合には保存は可能である。なお、使用中のアプリケーション・プログラムにより著作権データ以外のデータDを表示・印刷・保存・複写・加工・転送することが可能なことはいうまでもない。

【００３４】この図において２１は１次ユーザの装置２０内に内蔵された不揮発性半導体メモリあるいはハード・ディスク・ドライブ等の記憶装置、２２は出力用の表示装置、２３は出力用の印刷装置、D1は１次著作権データ、Dは一般データ、２４はフレキシブルディスクあるいはCDROMによる複写、ネットワークシステムによる転送でデータを供給される２次ユーザである。なお、この図において実線で示されたのは許される処理経路、点線で示されたのは許されない処理経路である。

【００３５】１次ユーザ１３が外部の情報提供者１５あるいは１６から、直接にあるいはデータベース１１を介して入手した暗号１次著作権データED1iはともに供給される平文１次著作権ラベルLC1と組み合わされて１次ユーザ装置２０の記憶装置２１に格納される。記憶装置２１に格納されている暗号１次著作権データED1iの１次利用を希望する１次ユーザ１３は著作権管理プログラムPCにより暗号１次著作権データED1iの概要説明および暗号１次著作権データED1iが使用しているアプリケーション・プログラムの情報等が表示された平文１次著作権ラベルLC1を参照し、暗号著作権１次データED1i作成に使用されているアプリケーション・プログラムの有無等この暗号著作権１次データED1iの使用環境を確認する。

【００３６】その結果、暗号著作権１次データED1iの利用が可能であると判断され、１次利用者１３がこの暗

号１次著作権データＥＤ1iを使用することを著作権管理プログラムＰＣに入力すると、著作権管理プログラムＰＣは暗号１次著作権データＥＤ1iが使用しているアプリケーション・プログラムを起動し、暗号１次著作権データＥＤ1iを記憶装置２１から装置内のメモリに読み込む。その一方、平文１次著作権ラベルＬＣ1が鍵管理センタ１２に送られ、その結果、前に述べた処理フローにしたがい１次利用鍵Ｋ1が供給されると、１次利用鍵Ｋ1に含まれている１次暗号鍵Ｋ1iを用いて暗号１次著作権データＥＤ1iが平文１次著作権データＤ1iに平文化され、

Ｄ1i＝Ｄ（Ｋ1i，ＥＤ1i）

起動されたアプリケーション・プログラムによって使用することが可能となる。

【００３７】装置２０のメモリ上の平文１次著作権データＤ1iを記憶装置２１に保存する場合には第１暗号鍵Ｋ1iを用いて暗号化して、

ＥＤ1i＝Ｅ（Ｋ1i，Ｄ1i）

保存が行われる。この保存には、データ保全のための一時的ファイル（Temporaly File）の作成・保存も含まれる。再暗号化されたデータＥＤ1iを再利用する場合には第１暗号鍵Ｋ1iを用いて再復号化および再暗号化が行われる。なお、平文１次著作権データＤ1iあるいは暗号１次著作権データＥＤ1iの表示・印刷、保存あるいは加工以外の利用形態すなわち外部記憶媒体への複写および他の装置への転送は著作権管理プログラムＰＣにより禁止される。

【００３８】前に述べたように本発明のデータ著作権管理システムにおいて、入手した著作権データは通常の利用形態すなわちデータを表示装置２２に表示することによって直接的な利用を行うことおよびその利用結果をプリンタ２３で出力することに限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての２次ユーザ２４への転送および加工を行うことはできない。したがって、１次著作権データＤ1iの１部を切り出して他のデータＤに張り付けること（Cut & Paste）および他のデータＤの１部を切り出して１次著作権データＤ1iに張り付けることは著作権管理プログラムによって禁止される。また、１次著作権データＤ1iは第１暗号鍵Ｋ1iを用いて暗号化された状態ならば例外的に記憶装置２１に保存することができるが、何らかの加工が行われた場合に保存は禁止される。

【００３９】本発明のデータ著作権管理システムにおいて、１次著作権データＤ1と一般データＤとの区別および著作権データが加工されたか否かは、著作権管理プログラムＰＣが判別する。コンピュータファイルはファイル本体とそのファイルの属性を記述した管理テーブルから構成されている。したがって、この管理テーブルを調べることによりそのファイルが著作権データであるか否かが判別される。また、この管理テーブルにはファイルサイズ、作成日付が記入されており、これらを調べることによりファイルの加工が行われたか否かが判別される。

【００４０】記憶装置２１に保存されているときに１次著作権データＤ1iは暗号化されて１次著作権ラベルＬＣ1と結合されているが、メモリ上に読み込まれたときには著作権管理プログラムにより１次著作権データＤ1iと１次著作権ラベルＬＣ1は分離され、分離された著作権ラベルＬＣ1は著作権管理プログラムＰＣにより管理される。著作権管理プログラムＰＣは１次著作権データＤ1iがどのアプリケーション・プログラムによって使用されているかを監視し、１次著作権データＤ1iの一般データＤへの切り出し／張り付けおよび一般データＤの１次著作権データＤ1iへの切り出し／張り付けが行われることを禁止する。

【００４１】図４に示されたのは、本発明において著作権管理プログラムＰＣが行うデータ加工利用の制限を説明する概念図である。１次利用の結果、平文１次著作権データＤ1iの加工を行うことが適切であると判断されたとき、１次ユーザ１３は平文１次著作権データＤ1iの加工を行うことをネットワークシステム１４を経由して鍵管理センタ１２に対して通知する。

【００４２】平文１次著作権データＤ1iの利用を希望する１次ユーザ１３は平文１次著作権データＤ1iの加工を行うための２次利用鍵Ｋ2の配布をネットワークシステム１４を経由して鍵管理センタ１２に要求する。２次利用鍵Ｋ2の配布要求を受けた鍵管理センタ１２は２次利用鍵Ｋ2をネットワークシステム１４を経由して１次ユーザ１３に配布する。このことにより１次ユーザ１３の装置２０は加工モードになり、１次ユーザ１３は１次著作権データの加工が可能になる。

【００４３】１次ユーザ１３は暗号１次著作権データＥＤ1iを第１暗号鍵Ｋ1iで平文１次著作権データＤ1iに平文化した上で表示装置２３に表示してデータの加工を行うが、初めに１次著作権データの著作権を保護するために加工用平文１次著作権データＤ1iの複写が行われ、この複写によって得られた加工用平文１次著作権データＤ1i′に対して加工が行われる。この加工用平文１次著作権データＤ1i′あるいはこの加工途中の平文１次著作権データＤ1i″をユーザ１３の装置内に保存する場合には２次利用鍵Ｋ2により暗号化されて、

ＥＤ1i′＝Ｅ（Ｋ2，Ｄ1i′）

または　ＥＤ1i″＝Ｅ（Ｋ2，Ｄ1i″）

保存が行われる。暗号１次著作権データＥＤ1iは加工されることなく記憶装置２１内に保存されており、その管理テーブルと加工された加工用平文１次著作権データＤ1i′あるいはＤ1i″のファイルサイズ、作成日付を調べることによりそのファイルが加工されたファイルであるか否かが判別される。

【００４４】データの加工が終了するとそのデータは新規な複数の平文２次著作権データＤ2jとなり、これらの

データD2jについて新たに２次著作権が発生する。この２次著作権を保護するために平文１次著作権D1を加工した１次ユーザ１３は鍵管理センタ１２に対して第３暗号鍵K3jの配布を要求し、第３暗号鍵K3jの配布要求を受けた鍵管理センタ１２は、第３暗号鍵k3jをネットワークシステム１４を経由して１次ユーザ１３に配布する。第３暗号鍵K3jの配布を受けた１次ユーザ１３は、この第３暗号鍵K3jを用いて平文２次著作権データD2jを暗号化し、

ＥD2j＝Ｅ（K3j，D2j）

１次ユーザ１３の記憶装置２１内には暗号化データＥD2jが保存される。この暗号化データＥD2jを利用する場合には第３暗号鍵K3jを用いて復号化および暗号化が行われる。

【００４５】１次ユーザ１３により加工された平文２次著作権データD2jには、情報提供者が有する加工される前の平文１次著作権データD1iの１次著作権に加えて、データ加工についての２次著作権が存在する。この２次著作権を行使するために１次ユーザ１３は鍵管理センタ１２に３次暗号鍵K3jとともに、データのタイトル名，使用しているアプリケーション・プログラム名，内容概要，１次著作権者名を送り、鍵管理センタ１２は３次暗号鍵K3jとともに保管し、管理する。

【００４６】一方、１次ユーザ１３は暗号化された２次著作権データＥD2jを外部記憶媒体１８への複写あるいはネットワークシステム１４を介して転送することにより２次ユーザ２４へ供給する。

【００４７】供給された暗号２次著作権データＥD2ｊの利用を希望する２次ユーザ２４は、鍵管理センタ１２に３次暗号鍵K3jの配布を要求する。この３次暗号鍵K3jによる平文２次著作権データD2ｊの利用は平文２次著作権データD2jの一般的な利用及びユーザ装置内への保存に限定され、平文２次著作権データD2jあるいは暗号化２次著作権データＥD2jの外部記憶媒体１８への複写あるいはネットワークシステム１４を利用することによる３次ユーザへの転送及び平文２次著作権データD2jの加工を行うことはできない。

【００４８】前に述べたように、本発明において扱う著作権データはプログラムとデータが一体化した「オブジェクト」を対象としており、このオブジェクトはコンピュータプログラミングあるいは各種処理において部品的な取り扱いをすることができる。図５および図２により、オブジェクトである複数の著作権データを利用して新しい著作権データを作る場合について説明する。図５において、３１，３２，３３は各々オブジェクトとして構成された著作権データD11，D12，D13であり、これらの著作権データD11，D12，D13を利用して新しい著作権データD2j３０が作成される。著作権データD11，D12，D13の利用形態としては、３４に示された著作権データD11のようにその全部を利用する、３５に示された著作権データD12のようにその一部を利用するあるいは３６に示された著作権データD13のように修正して利用する、の３形態がある。

【００４９】著作権データの加工は、オブジェクト単位で著作権データをリンクして引用して重ね合わせ／組み合わせを行うことにより加工処理が行われ、このような重ね合わせおよび組み合わせは自由に行うことができる。また、このように重ね合わせ／組み合わせが行われた著作権データ３７にさらに他の事項を付け加えることもできる。このようにして新規に作成された著作権データD2jはオブジェクトの集合体として構成されている。

【００５０】このようにして作成された平文２次著作権データD2jには１次著作権データD1iの著作権の他に新たに加工を行った１次ユーザ１３の２次著作権が発生する。この２次著作権を行使するためには平文２次著作権データの暗号化が必要であり、そのために１次ユーザ１３は３次暗号鍵K3jを用意し、平文著作権データD2jを３次暗号鍵K3jを用いて暗号化し、

ＥD2j＝Ｅ（K3j，D2j）

外部記憶媒体１８への複写あるいはネットワークシステム１４を介して転送することにより２次ユーザ１９へ供給する。また、３次ユーザが３次暗号鍵K3jを容易に入手することができるように、鍵管理センタ１２に第３暗号鍵K3jを登録する。この第３暗号鍵K3jの登録により、１次ユーザ１３の２次著作権が鍵管理センタ１２に記録される。

【００５１】このとき１次ユーザ１３から鍵管理センタ１２に送られるのは、作成した複数の２次著作権データの数に対応した複数個の第３暗号鍵K3jの他に、第３暗号鍵K3jの数，２次暗号鍵K2i，使用した１次著作権データ，著作権管理プログラムがリンクしている他の著作権データの情報，使用した著作権データへのアクセスパス，使用した著作権データが使用しているアプリケーションプログラムおよび著作物説明文章等である。

【００５２】供給された暗号２次著作権データD2jの利用を希望する２次ユーザ１９は、鍵管理センタ１２に第３暗号鍵K3jの配布を要求する。第３暗号鍵K3jの配布要求を受けた鍵管理センタ１２は、第３暗号鍵K3jをネットワークシステム１４を経由して２次ユーザ１９に配布する。第３暗号鍵K3jを受け取った２次ユーザ１９は、第３暗号鍵K3jを用いて暗号２次著作権データＥD2jを復号・平文化し、利用する。

【００５３】著作権管理プログラムPCは、第３暗号鍵K3jを受け取ると、それぞれの著作権データD2jに著作権ラベルLC2jを付けて２次利用者が利用可能な状態にする。この時、新規作成の著作権データとリンクされていたオブジェクトである著作権データとのリンクが解除される。解除された時点で、リンク関係だけであった利用著作権データの実体が、新規著作権データＥD2jに埋め込まれ、ＥD2jファイルだけで著作物の流通が可能と

なる。この場合も、暗号著作権データＥＤ2jを再度利用する場合には第３暗号鍵Ｋ３ｊを用いて復号化および暗号化が行われる。

【００５４】鍵管理センターは、第３暗号鍵Ｋ３ｊを要求元に返送するとともに、著作権ラベルＬC1及びＬC2をもとに課金処理を行う。著作権データ所有者は、鍵管理センターに申請することにより自分の著作権データのアクセスパスを変更することができる。著作権データの所有者は、第３暗号鍵K3jで自分の著作権データを加工（修正）することも可能であり、さらに、別の鍵で登録することも可能である。

【図面の簡単な説明】

【図１】本発明が対象とするデータ著作権管理システムの構成図。

【図２】本発明のデータ著作権処理システム実施例の概要構成図。

【図３】本発明において著作権管理プログラムPCが行う１次利用の制限を説明する概念図。

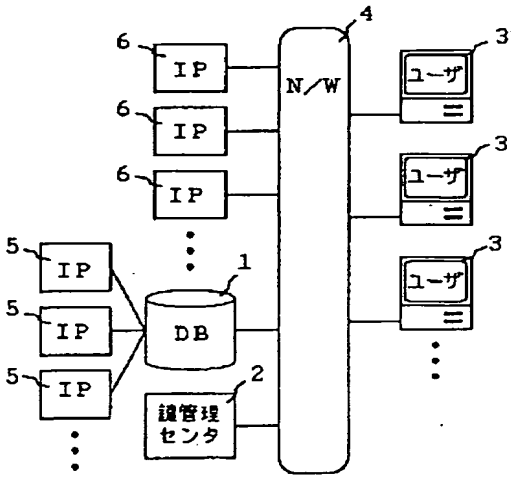
【図４】本発明において著作権管理プログラムPCが行うデータ加工利用の制限を説明する概念図。

【図５】オブジェクトである複数の著作権データを利用しての新しい著作権データ作成の説明図。

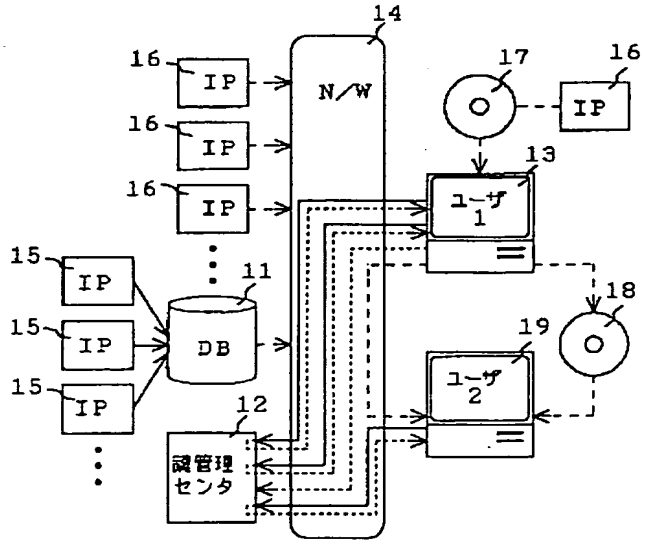
【符号の説明】

１，１１　データベース
２，１２　鍵管理センタ
３　ユーザ
４　ネットワークシステム
５，６，１５，１６　情報提供者
１１　データベース
１２　鍵管理センタ
１３　１次ユーザ
１４　ネットワークシステム
１７　情報記録媒体
１８　外部記憶媒体
１９，２４　２次ユーザ
２０　１次ユーザの装置
２１　記憶装置
２２　表示装置
２３　印刷装置
２４　２次ユーザ
３０　新しい著作権データ
３１，３２，３３　著作権データ
Ｄ　一般データ
D1　１次著作権データ
D1i　平文１次著作権データ
D1i′　加工用平文１次著作権データ
D2j　平文２次著作権データ
ＥD1i　暗号１次著作権データ
ＥD2j　暗号化データ
K1i　第１暗号鍵
K3j　第３暗号鍵
ＰＣ　著作権管理プログラム

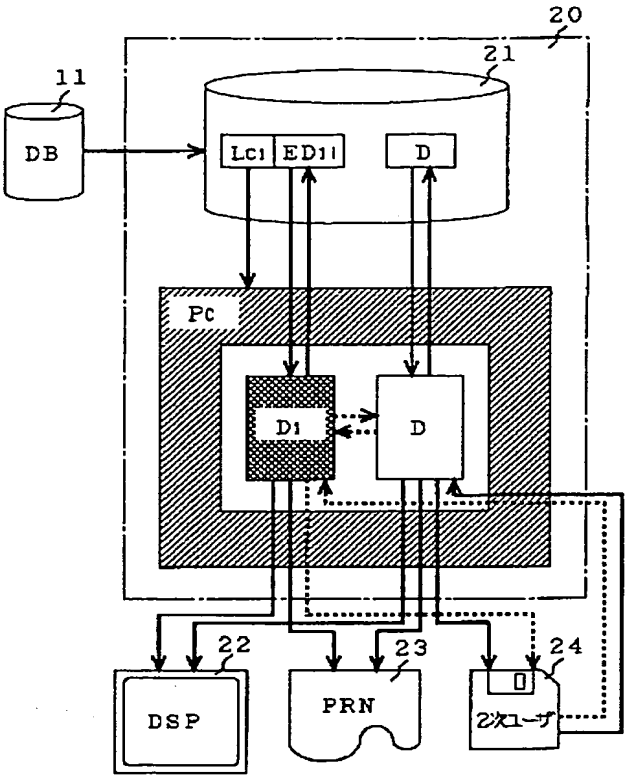
【図１】



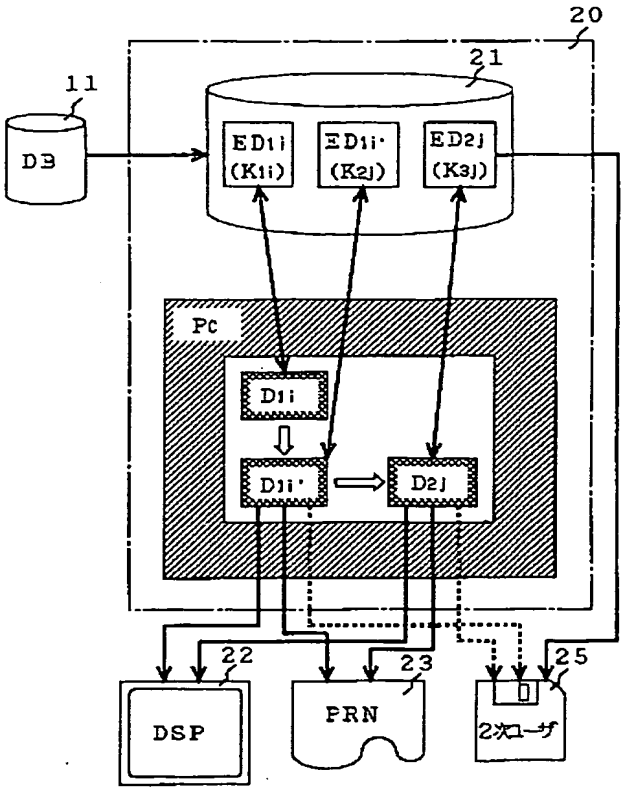
【図２】



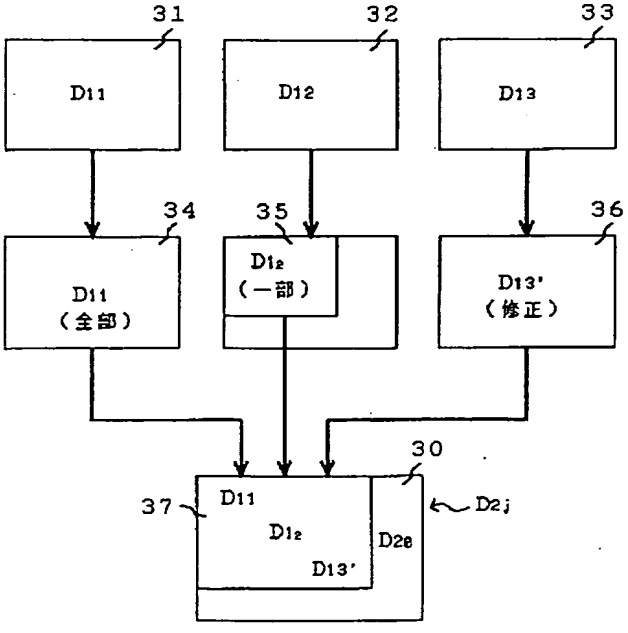
【図３】


20
21
11
DB
Lc1
ED11
D
Pc
D1
D
22
23
24
DSP
PRN
2次ユーザ

【図４】


20
21
11
DB
ED1i
(K1i)
ED1i'
(K2j)
ED2j
(K3j)
Pc
D1i
D1i'
D2j
22
23
25
DSP
PRN
2次ユーザ

【図５】


31
32
33
D11
D12
D13
34
35
36
D11
(全部)
D12
(一部)
D13'
(修正)
30
37
D11
D12
D13'
D2e
D2j

フロントページの続き

(51) Int.Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
H04L 9/14			H04N 7/167	
H04N 7/167				